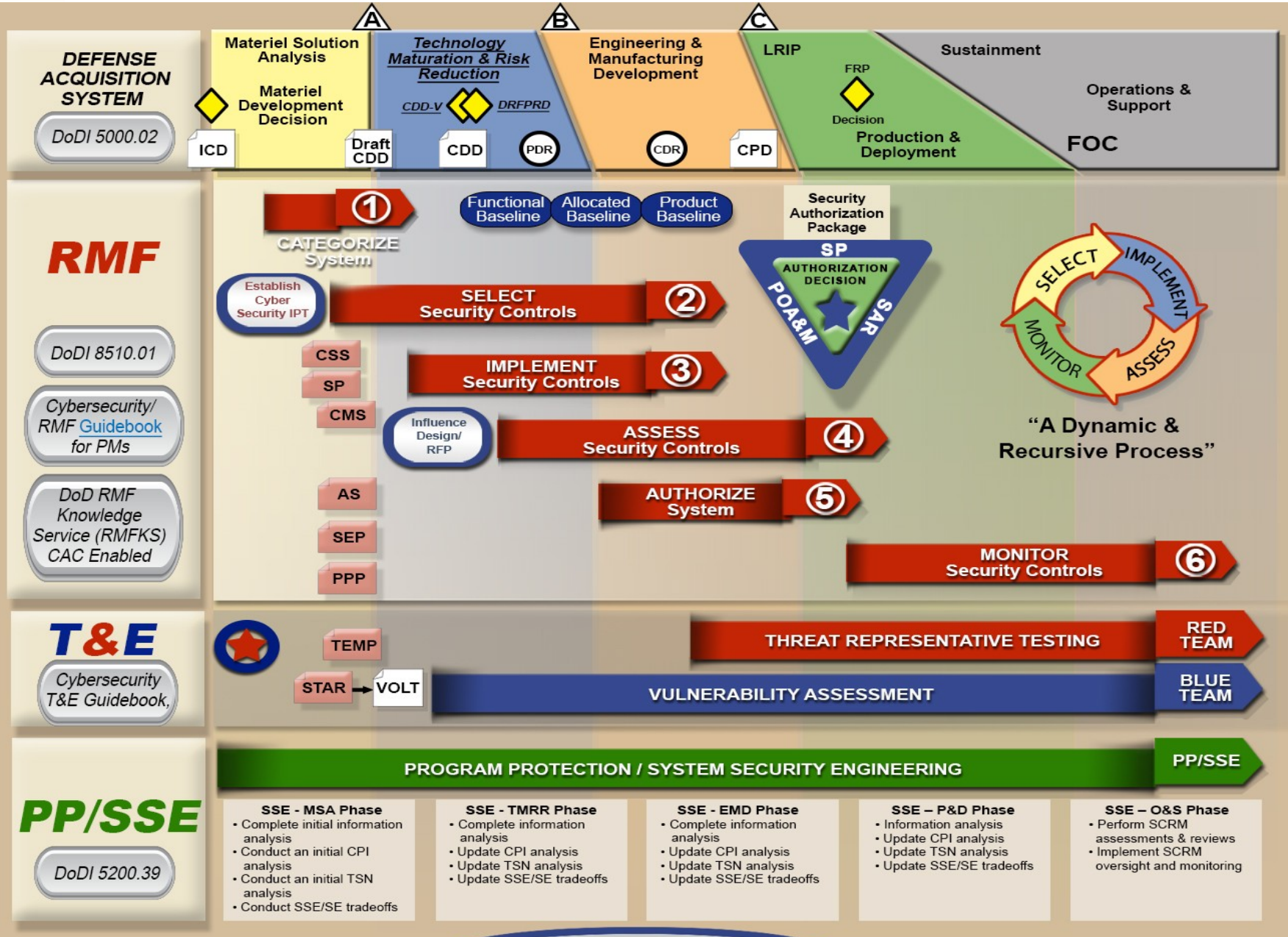
Integration of Cybersecurity & the Acquisition Lifecycle



E IN PRESENTATION MODE TO USE TOOL!

Questions that PMs need to ask

CALIT Ver 1.9

Program Protection (PP) Overview

- Program protection is the integrating process for managing security risks to DoD warfighting capability from:
  - Foreign intelligence collection
  - Hardware
  - Software
  - Cybersecurity vulnerability – **Yes, Cybersecurity is a subset of Program Protection!**
  - Supply chain exploitation
  - Battlefield loss throughout the system life cycle

- Program Protection focuses on two general threats:
  - Critical Program Information (CPI) compromise – CPI refers to *elements of U.S. capabilities that contribute to the warfighters' technical advantage, and that if compromised, undermine U.S. military preeminence."*
  - Malicious Insertion – The threat of Malicious Insertion is defined as "*unauthorized changes to system components with the intent to alter, degrade, or interrupt system performance, functionality and/or data*

- The Program Protection Plan (PPP):
  - Summari[illegible]ities for protectin[illegible]

Sources: **ACQ160 – Program Protection Planning Awareness Course**

Forward

Program Protection (PP) / Systems Security Engineering (SSE)

- Program Protection Planning defines the plan for and a summary of the results of the SSE effort

- SSE is the discipline that implements program protection

- SSE is a specialty discipline of systems engineering with several components:
  - **Cybersecurity – That's right, Cybersecurity is a form of Systems Engineering too!!**
  - Hardware Assurance
  - Software Assurance
  - Anti-tamper
  - Supply Chain Risk Management
  - Defense Exportability

- Program Protection Planning summarizes system security requirements as protection measures. Specifics of the protection measures for a program become the programs' SSE requirements

Sources: **ACQ160 – Program Protection Planning Awareness Course**

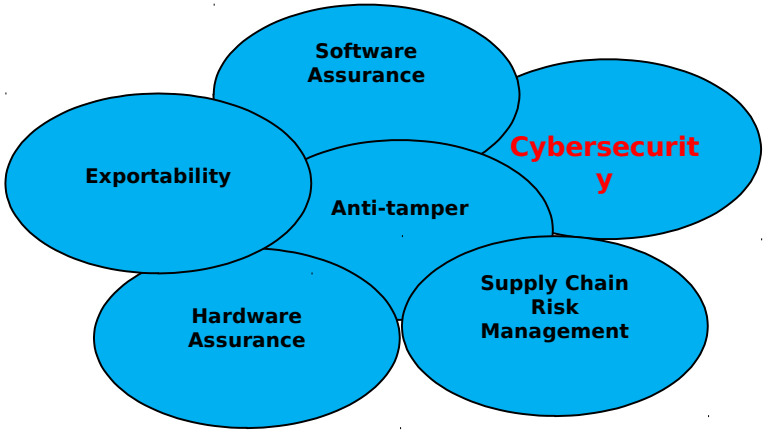
DAG Chapter 13.14 – Detailed System Security Engi

Back

Forward

The Systems Security Engineering (SSE) Specialties

- Each engineering specialty brings a perspective, methods, skills and protections that identify unique and overlapping requirements



- Integrated system security requirements need contributions from all of the security engineering specialties just as Systems Engineering needs contributions from reliability, safety, manufacturing and other specialties.

Sources: **ACQ160 – Program Protection Planning Awareness Course**

DAG Chapter 13.14 – Detailed System Security Engi

Back

Forward

Security Engineering Specialties Quick Reference

- **Cybersecurity**: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DoDI 8500.01)

- **Hardware Assurance**: The level of confidence that hardware, e.g., electronic components such as integrated circuits and printed circuit boards, functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware throughout the lifecycle.

- **Software Assurance:** The "Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle and that the software functions in the intended manner." (Public law 112-239-Jan 2013).

- **Anti-Tamper:** Systems engineering activities intended to prevent or delay exploitation of CPI in U.S. defense systems in domestic and export configurations to impede countermeasure development, unintended technology transfer, or alteration of a system due to reverse engineering.

- **Supply Chain Risk:** The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design integrity, manufacturing, production, distribution, installation, operation or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system (*National Defense Authorization Act for FY2011 Section 806*)

- **Defense Expo** rotection features into a sy[illegible] during its research and development phase. (*National*

Sources: ACQ160 – Program Protection Planning Awareness Course

Back

Forward

Approach to Integrating Systems Security Engineering (SSE) Requirements

SSE is a discipline which may be assigned to a Systems Engineer (SE) or a system security engineer (an SE trained in security engineering)

SSE reconciles and trades security engineering specialty requirements to ensure integrated, affordable security with acceptable risk

The SSE and SE responsibility is to get the selected set of security requirements incorporated into the system requirements document and the statement of work used for an RFP and contract.

The security requirements are of three types:

- Protection measures that say what the system does are system security requirements included in the System Requirements Document (SRD) and referenced by the PPP and the TEMP

- Protection measures that specify how the contractor will develop the system are included in the Statement of Work (SOW) and referenced by the PPP

- Program P[illegible] activities necessary to continue to assess

Sources: **ACQ160 – Program Protection Planning Awareness Course**

Back

Forward

Interrelationship of the SEP, PPP and TEMP

System Engineering Plan (SEP):

- Defines the SE organizational responsibilities for program protection planning
- Calls for program protection updates as entrance criteria for all SE technical reviews
- Provides a schedule of PMO SE activities

Program Protection Plan (PPP):

- Summarizes the planned PMO's security protection activities for protecting the system during design and development
- Contains the results of the PPP analysis identifying the key elements of the program which require protection
- Summarizes the System Requirements Document (SRD) and Statement of Work (SOW) system security requirements as protection measures

Test and Evaluation Master Plan (TEMP):

- Contains verification and validation plan of the system security requirements
- Contains a schedule of testing and test events

Collectively, t n systems that perform a required with the Program protection

Sources: **ACQ160 – Program Protection Planning Awareness Course**

Back to Previou

Back to Map

Questions PMs Can Ask to Determine if Cybersecurity is Integrated into Defense Acquisition Programs

- PMs and Defense Acquisition Workforce Members in General can get a sense of the extent of successful integration of Cybersecurity into their Defense Acquisition Programs by asking the right questions

- The *DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) in the System Acquisition Lifecycle, Version 1.0, May 26, 2015* provides a list of questions PMs can ask to determine if this integration is taking place. These questions can be found on **pg 140** of this document.

Back